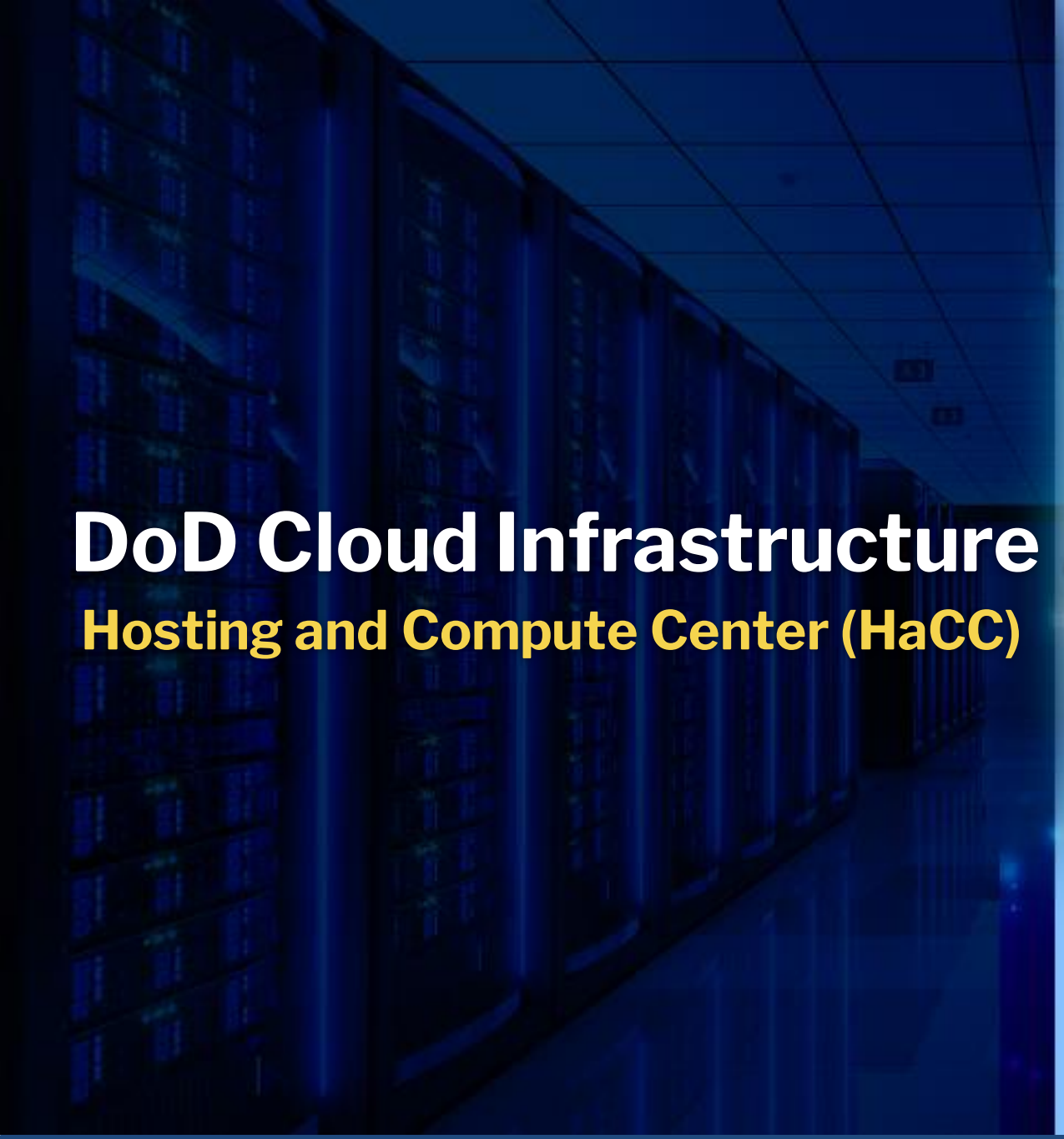


DoD Cloud Infrastructure As Code (IaC)

Hosting and Compute Center (HaCC)

Mr. David Lago

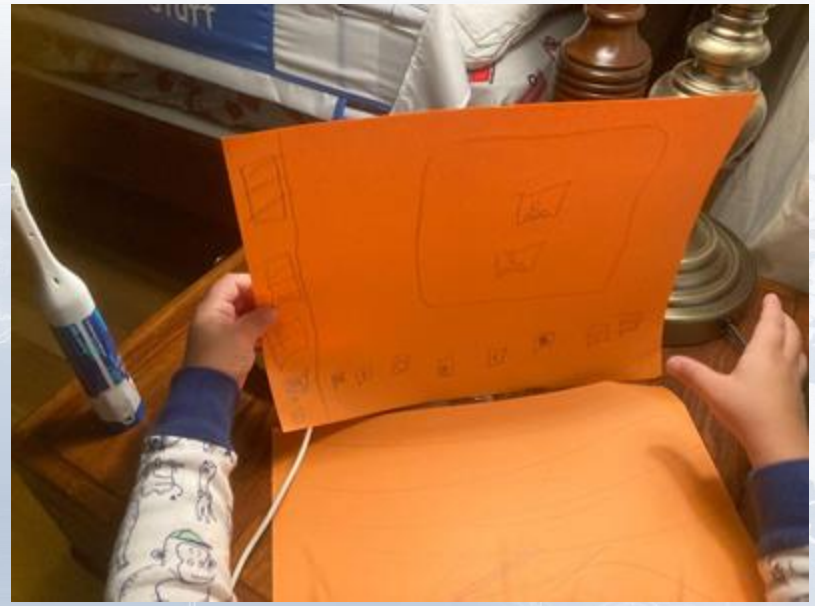
Product Manager

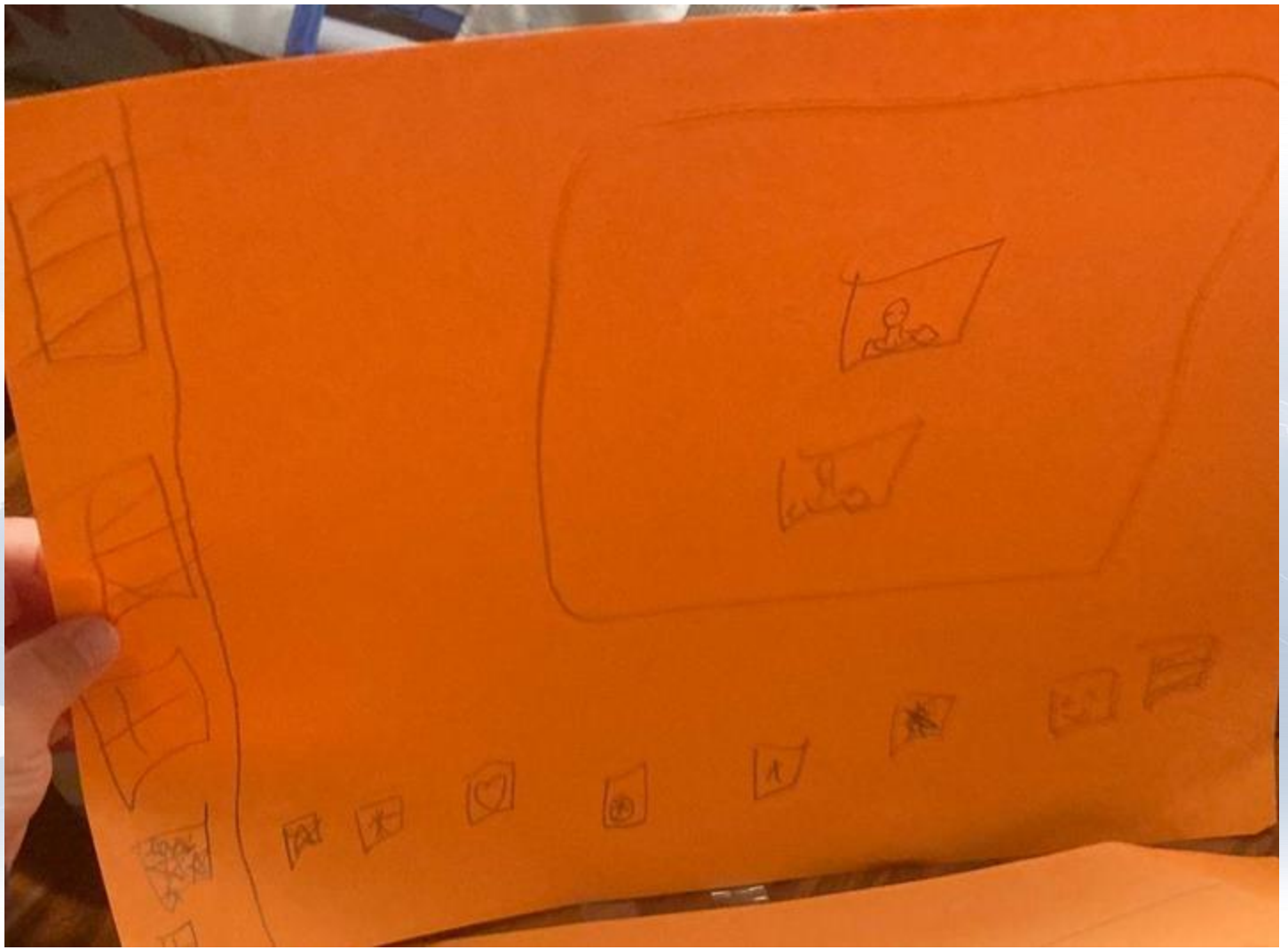
28 October 2021

DISCLAIMER

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

Cloud Shouldn't be an Uphill Journey





Cloud Shouldn't be an Uphill Journey

BLUF - DoD Cloud IaC

Builds cloud environments through automation; takes 7 months off typical cloud journey.

- Partnership between CCPO and DCIO IE
- Baselines for both Azure and AWS *(3rd CSP coming in FY22)*
- Supports IL2, IL4 and IL5 workloads. IL6 in work

- Only decentralized IaC baseline with ATO; 132 Common Controls
- Only IaC baseline available in Azure Marketplace
  - AWS Marketplace planned for FY22
- Only IaC baseline developed under CRADAs w CSPs
  - We will help deploy baseline in one 3-4 hour session for free
  - Completed deployments for 13 DoD orgs

What is DoD Cloud IaC?

DoD Cloud IaC are baselines that leverage IaC automation to generate **pre-configured, pre-authorized, Platform as a Service (PaaS)**-focused environments. Whenever possible, DoD Cloud IaC leverages security services offered by Cloud Service Providers (CSP) over traditional data center tools. DoD Cloud IaC helps customers adopt cloud faster.

Azure App Service

Azure Kubernetes Service

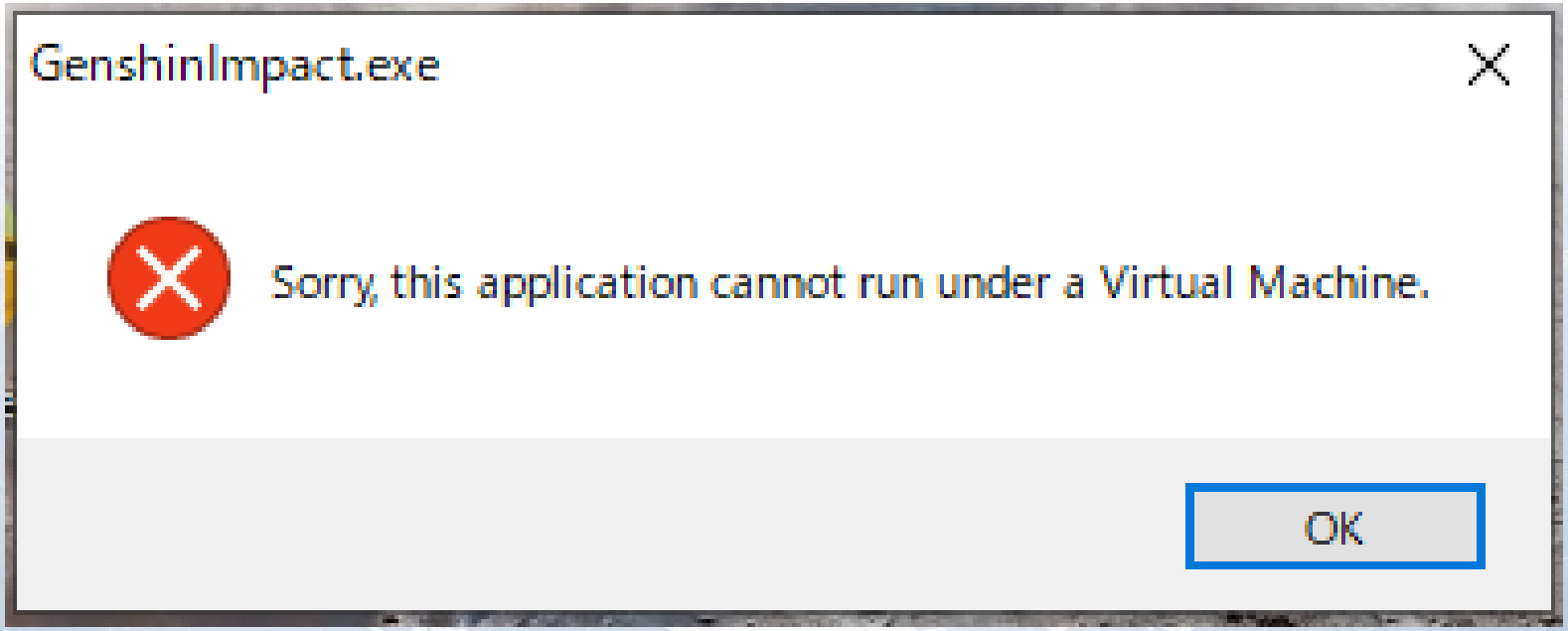
Azure Sentinel

AWS Elastic Kubernetes - Fargate

AWS Guard Duty

AWS Aurora

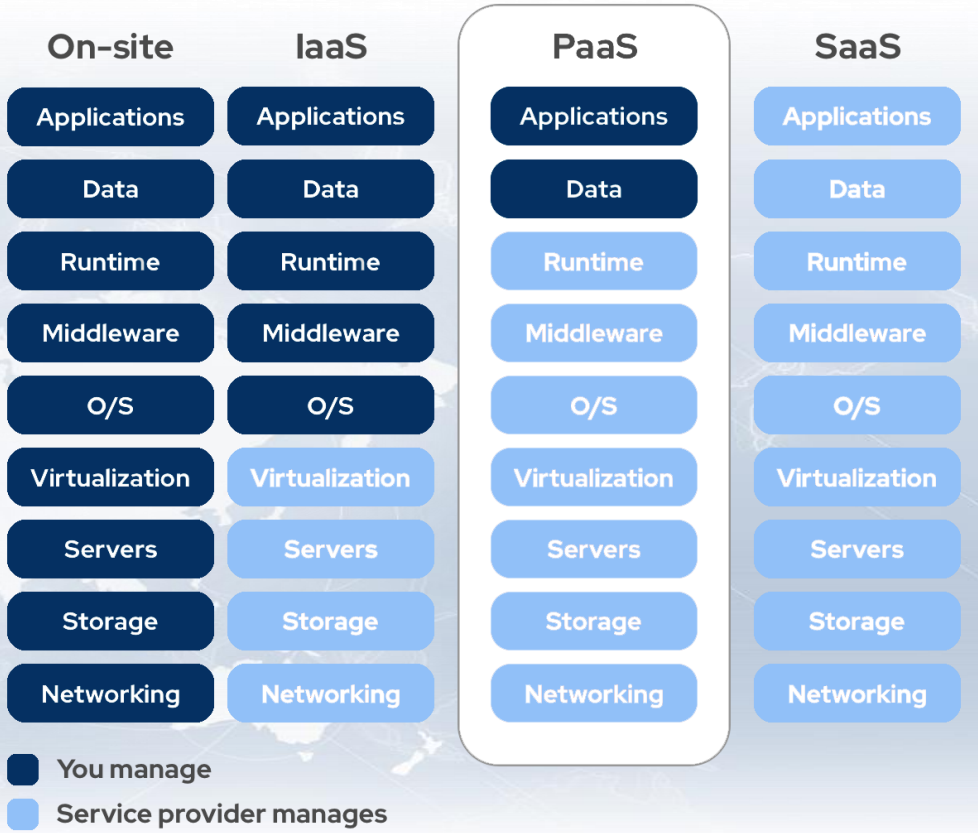
DoD Running to PaaS & SaaS



Traditional IaaS Shared Responsibility Model (SRM)
6% IaaS CSP Common Controls, 94% Mission Owner Responsibility

Why CSP Platform as a Service (PaaS)?

- Patching is the responsibility of the CSP (No ACAS)
- Host-based security is the responsibility of the CSP (No HBSS)
- Hardening is mostly CSP responsibility (Minimal STIGs/SRGs)
- Middleware integration is the responsibility of the CSP
- PaaS offerings are the focus of cloud innovation



PaaS Examples

- Azure Database: SQL
- Azure App Service – App Hosting
- Azure Functions – Serverless (Backlog)
- Azure Kubernetes Service – Containers
- Azure IoT– Internet of Things
- Azure PlayFab – Game Engine
- Azure Quantum – Quantum Computing
- AWS Relational Database Service
- AWS Elastic Beanstalk
- AWS Lamba – Serverless
- AWS Kubernetes Service – Serverless
- AWS Greengrass - Internet of Things
- AWS Lumberyard – Game Engine
- AWS Bracket – Quantum Computing

Not Traditional Compliance and That's Fine

Each Baseline Consists of…

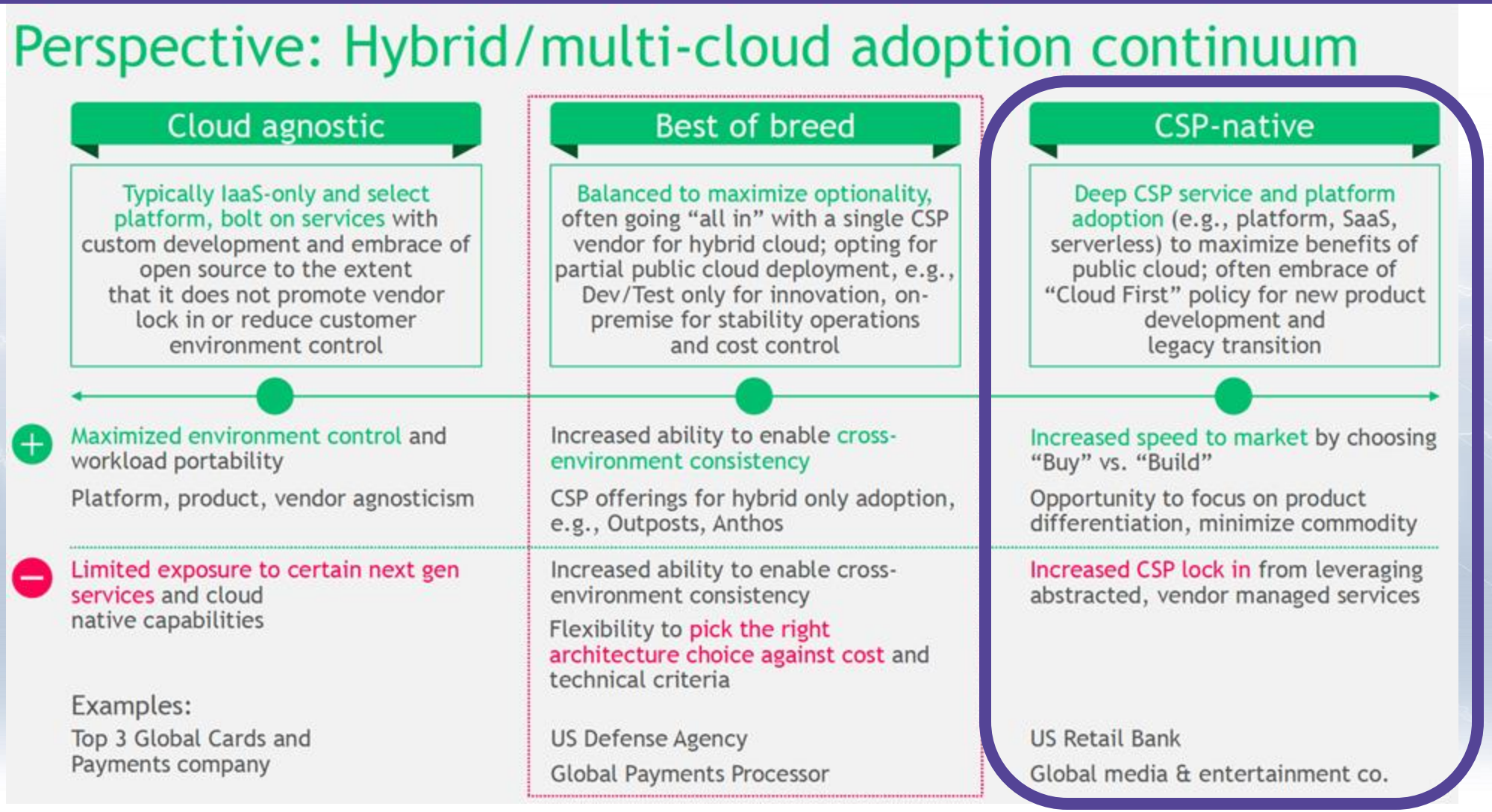
IaC Templates

Least Privilege Model

Security Policies

CAC Authentication w/ DISA Global Directory

Follows a CSP-Native Approach



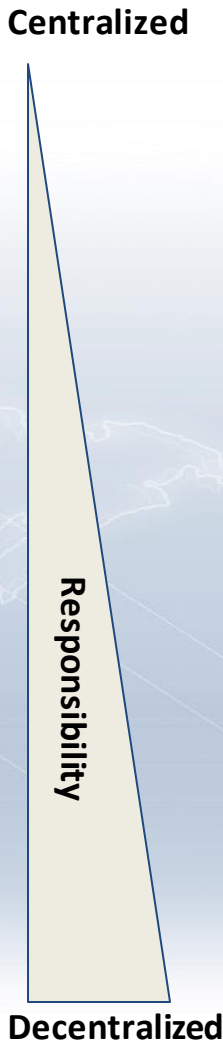
Source: Boston Consulting Group

DoD Cloud IaC - Consumption Options

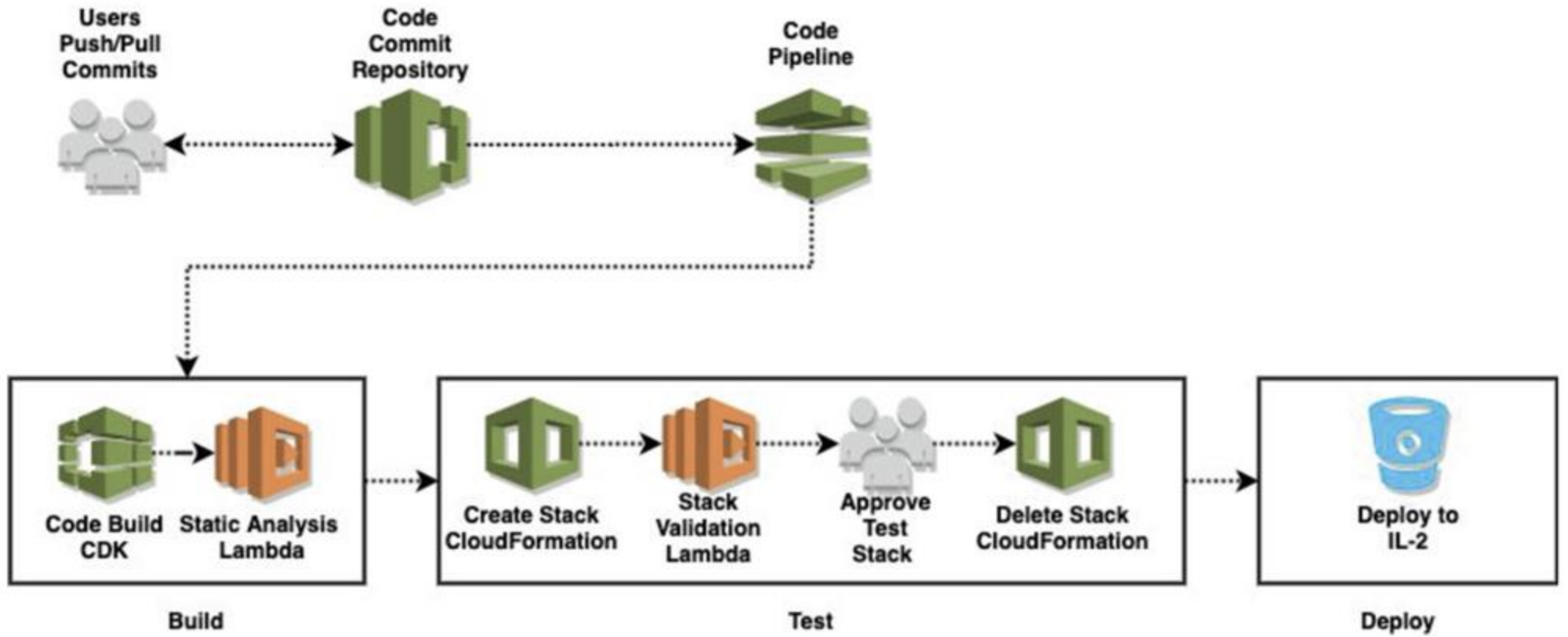
- **Baked into a Platform:** Incorporating elements of the DoD Cloud IaC baseline (e.g. Security Policies, PaaS IaC) and offering as part of a larger platform

- **Peered to SCCA Provider:** Building the environment using DoD Cloud IaC baseline and then peering to an existing SCCA provider for VDSS and VDMS services leveraging a Cloud Access Point (CAP)

- **Decentralized Cloud Operator:** Deploying the DoD Cloud IaC baseline to their own tenant. Provides VDSS and VDMS services locally using DoD Cloud IaC CSP native security services, including CSSP integration. Can operate on DODIN w/ a CAP or on Internet w/ a Cloud Native Access Point (CNAP)

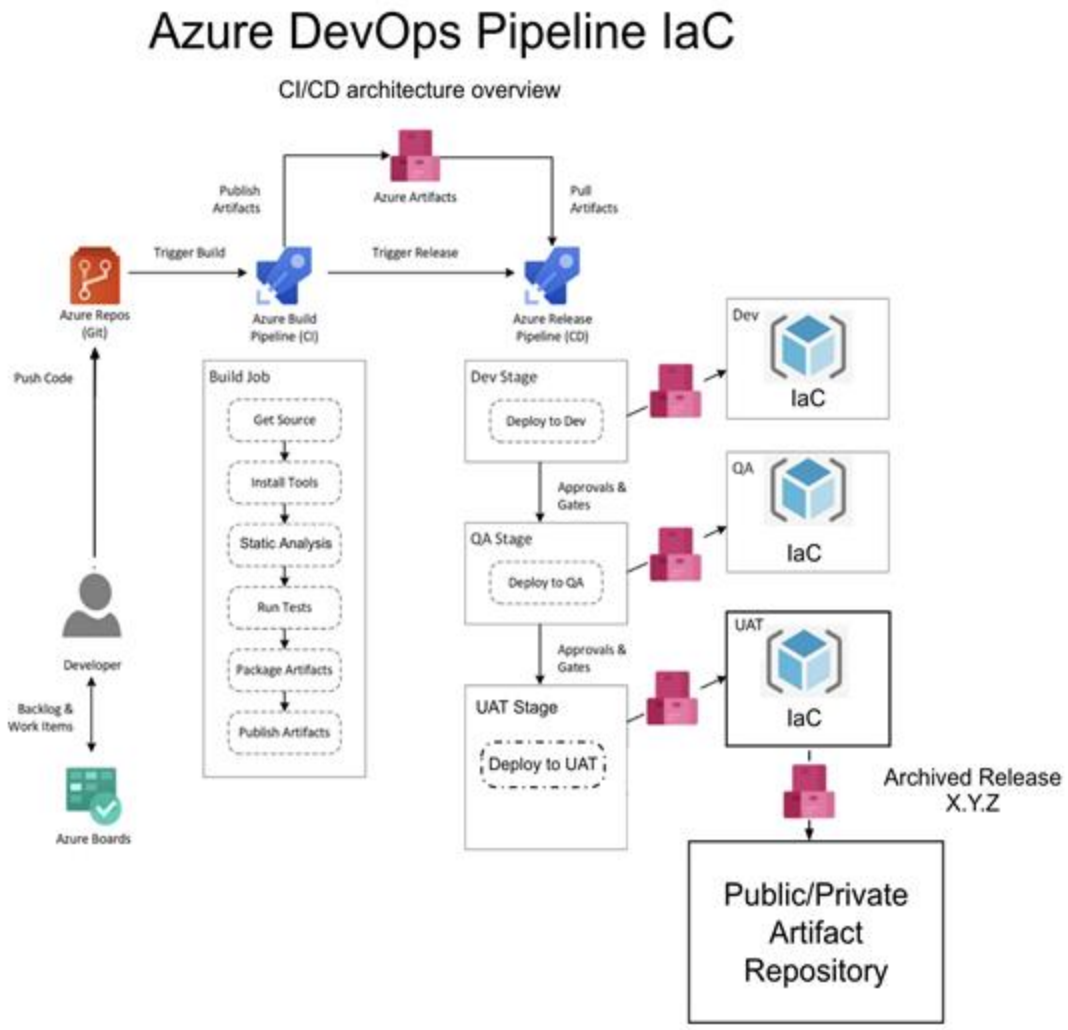


DoD Cloud IaC for AWS - CI/CD



DoD Cloud IaC for Azure CI-CD

- Leverages Azure DevOps (ADO)
- Planning for Github AE if available at reasonable cost
  - GitHub AE currently has a 500-user minimum per instance
  - Does not fit DoD Cloud IaC low-cost, small team model



IaC in Use: Blue Heron C2 System for OAR

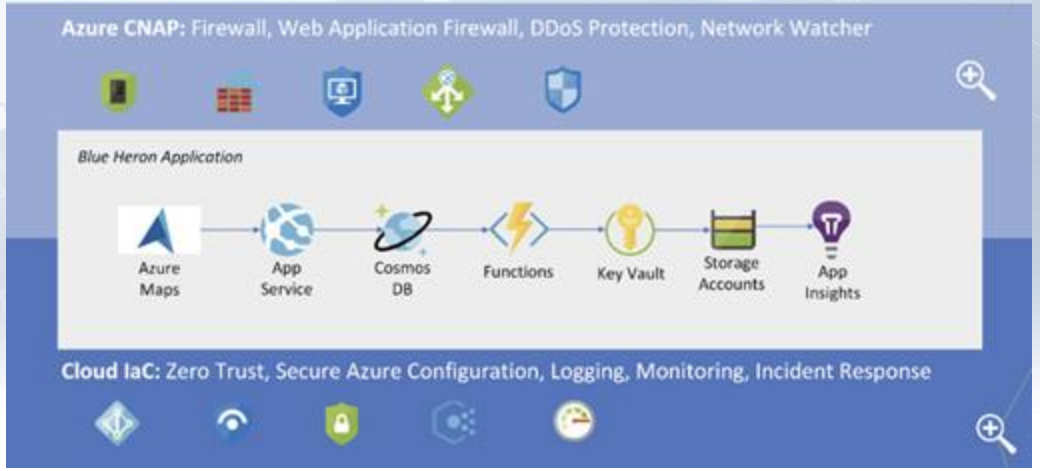
TRANSCOM Air Mobility Command (AMC) built a Command and Control (C2) system in 16 days w/ 3 FTE and a 10k budget to support OPERATION ALLIED REFUGE in Afghanistan

The DoD Cloud IaC for Azure baseline was used to deploy a serverless architecture to scale from pilot to production in 72 hours

IaC in Use: Blue Heron Architecture

- Azure Maps - Geospatial visualization
- Azure Firewall & Azure Web Application Firewall - Network Defense & CNAP
- Azure Active Directory w/ Global Directory - Authentication
- Azure App Service, Azure Functions, Azure SignalR - App Hosting
- Azure Cosmos DB & Azure Redis - Database hosting

Azure Maps



Closing

Take a "PaaS-First" approach

Lean forward don't build yesterday's Landing Zone tomorrow

Don't start from scratch

Leverage existing platforms or IaC baselines; use that savings to improve the mission app

Free the cloud!

Give mission owners options to improve technology to the warfighter

Contact Us

Looking for more on IaC? Connect with the HaCC today…

www.HaCC.mil

Closing Slide

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

/DISA **@USDISA** **/USDISA** **DISA.mil**